The internet and private life in Europe

Dinant, Jean-Marc; Poullet, Yves

Published in:
New dimensions in Privacy Law

Publication date:
2006

Document Version
Publisher's PDF, also known as Version of record

4

The internet and private life in Europe: Risks and aspirations

YVES POULLET WITH THE COOPERATION OF J. MARC DINANT

Introduction

The reach of the internet grows day by day. Currently there are over 2 billion users and the number continues to rise. The services offered on the internet follow the same exponential trend. Electronic commerce promises ever more varied and ingenious applications, putting the world at one's fingertip with a simple click. Nevertheless concerns have been raised about this virtual universe bringing about the end of our freedoms, especially with respect to privacy. The purpose of this chapter is to bring clarity to the debate and to offer some suggestions. The topic is a timely one in Europe. There are now two European Directives on privacy protection, in particular the general Data Protection Directive 95/46/EC of 24 October 1995[1] and the more specific Privacy and Electronic Communications Directive 2002/58/EC of 12 July 2002.[2] The latter replaces the Directive 97/66/EC of 15 December 1997 on the processing of personal

This chapter is a deeply updated version of an article by the first author originally published in the French language under the title 'Internet et Vie Privée: Entre Risques et Espoirs' in (2001) *Journal des Tribunaux* 155. Translation, Dr Martin Vranken, Law Faculty, University of Melbourne. It also takes into account the report prepared by the two authors for the Council of Europe Consultative Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Yves Poullet and J. Marc Dinant, *Information Self-Determination in the Internet Era: Thoughts on Convention No. 108 for the Purposes of the Future Work of the Consultative Committee*, 13 December 2004 (T-PD (2004) 04 final).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995, *OJ*, L 281, 23 November 1995.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002, *OJ*, L 201, 31 July 2002. On that directive, see Sophie Louveaux and Maria Veronica Perez-Asinari, 'New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communication

data and the protection of privacy in the telecommunications sector.[3] A large number of documents generated within the European Community also are topical – including the European Parliament's 1999 report on Echelon;[4] the European Commission's consultation paper on the surveillance by companies of employee internet use;[5] the European Commission's communication on spam;[6] and finally the Council Framework Draft Decision on Data Retention.[7] In addition, one has to mention the important work done by the Article 29 Data Protection Working Party on various privacy issues in order to harmonise the different national approaches.[8]

Which specific characteristics of the network account for the current controversy surrounding the internet and privacy?[9] Five features in

Sector – Some Initial Remarks' (2003) 6(5) *Computer and Telecommunications Law Review* 133.

[3] Directive 1997/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, *OJ*, L 024, 30 January 1998.

[4] European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system)*, 2001/2098(INI).

[5] European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (30 October 2002). See also EIRO (European Industrial Relations Observatory Online), Catherine Delbar, Marinette Mormont and Marie Schots, *Comparative Report on New Technology and Respect for Privacy at the Workplace*, TN0307101S, 12 August 2003, available from http://www.eiro.eurofound.ie/index.html.

[6] European Commission, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Unsolicited Commercial Communications or 'Spam'*, COM(2004) 28, 22 January 2004.

[7] Council of Europe, *Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the Purpose of Prevention, Investigation, Detection and Prosecution of Crime and Criminal Offences including Terrorism*, 8958/04, CRIMORG 36, TELECOM 82, 28 April 2004. This draft intends to harmonise in the context of the third pillar the European national regulation on traffic data retention for criminal investigation purposes.

[8] This group – commonly known as the Article 29 Working Party – was set up under Directive 95/46/EC, Art. 29 as an independent European advisory body compounded by representatives of the different national data protection authorities. Its report covers the years 2002 and 2003: European Commission, *Seventh Report on the Situation regarding the Protection of Individuals with regard to the Processing of Personal Data and Privacy in the European Union and in Third Countries* (Luxembourg: Office for Official Publications of the European Communities, 2004) (report adopted on 21 June 2004).

[9] In the context of this chapter, we do not take into consideration the development of new terminal equipment like Radio Frequency Identifier (RFID) which are very small chips embedded in goods (e.g. shirts or razors) or human beings and permit the tracking of their movements. About this new phenomenon and the new privacy threats linked with their use, see Article 29 Working Party, *Working Document on Data Protection Issues related to RFID Technology*, 10107/05/EN, WP 105, 19 January 2005.

particular stand out and warrant close attention.[10] First, there is the interactive nature of the internet, which over time leads to the generation of a vast array of person-specific information. As internet use is interactive and increasingly a part of everyday life, users themselves are the primary creators of data, whenever they enter into a dialogue with a particular website, when driving their car equipped with a global positioning system, or simply when using a mobile phone linked to the internet. All such activities leave traces, made consciously or unconsciously, and these are captured by others in order to enrich or even create various applications. Further, because of the interactive nature of the internet, users can make choices at all times: by discontinuing their visit to a particular site; by choosing whether or not to identify themselves; by insisting on this or that protection; by consenting to this or that treatment. Consent is the corollary of interactivity. It constitutes a major factor in the safeguarding of our freedoms on the internet, a point I will come back to later in this chapter.[11]

The second characteristic is the combination of flow rate and processing power increase. According to the current state of the art, fibre optic cables, which are insensitive to electromagnetic interference, permit flow rates of the order of 10Gbits/second.[12] Present day cables contain several fibres (from a few dozen to a few hundred). Thanks to DSL technology, it is normal to achieve flow rates of up to four megabits a second without having to modify the conventional twisted pair telephone wire and with equipment costing less than a hundred euros. This means it will become technically possible for television to be distributed via the internet rather than satellite or a dedicated coaxial cable. Experiments along these lines are under way in a number of countries. This presents a new challenge. At the moment, satellite and cable distribution technically do not, or hardly, enable the broadcaster to know what programmes the consumer is watching – all the signals arrive at the terminal device of the subscriber, who chooses what to watch. In the case of internet television, it will be possible to find out what each individual is watching and even insert advertising targeted at him or her at precisely chosen moments.

[10] As regards a more comprehensive description of the new technological landscape and its evolution, see Poullet and Dinant, *Information Self-Determination in the Internet Era*, unnumbered note on p. 60, above.

[11] See below n. 32 and following text.

[12] This refers to the equipment currently installed. Prototypes enable much faster speeds to be achieved.

Processing power has increased in correlation to the power and capacity of computer components. In 1987, a typical PC had an 8 MHz processor with 640 KB of random access memory and a hard disk of 20 megabytes. In 2004, a computer typically on sale in supermarkets had a 2.4 GHz processor (3,000 times more), 256 MB of RAM (400 times more) and a hard disk with a capacity of 60 GB (3,000 times more). Moreover, at equivalent speed, modern processors are significantly more powerful than their predecessors. There is an increasing tendency for computers to contain a greater number of processors, some of which play a more specialised role controlling a specific task (for example, display or the transmission and reception of signals on the network).[13] Certain processes, which used to be impossible, are now becoming perfectly feasible. The sampling and digitisation of a voice or an image can now be done in real time, with the result being of a quality very close to the original. Thus, it will become more and more possible and less expensive to record the lives of all individuals on the planet.[14]

The third characteristic of the internet is the open nature of the network and the associated range of available applications. Openness, in the sense that anyone can log on anywhere at any time, raises questions about the confidentiality of the messages circulating on a network that is not quite secure.[15] Openness also means that messages placed on the internet, say one's curriculum vitae or publications listed on it or even one's photograph, can be retrieved thanks to the power of a search engine and subsequently used for a different purpose – a purpose that may be uncontemplated at the time the information was put on the internet originally. Additionally, in travelling from one point to another on the internet, one can 'jump' endlessly from one site to the next producing a multitude of traces in different places in the process.

The global dimension of the network and the multitude of transborder movements give rise to unease regarding the privacy implications

[13] E.g. ASIC chips (or Application Specific Integrated Circuits) which are processors specially designed for a specific task (e.g. the digitisation of an analogue signal, encryption or decryption). Typically, an ASIC chip will run approximately one hundred times faster than a non-application-specific processor to carry out a particular task.

[14] Just one example: The Belgian National Register, which contains the demographic details of all Belgians from their birth to their death as well as their occupations, marriages and death and successive addresses (not counting the data on foreign residents in Belgium) would today easily fit onto a DAT cassette the size of a large box of matches or on a few DVDs. It could be transmitted in its entirety by fibre optic cable in less than a minute.

[15] The anticipated generalised use of cryptic systems certainly would be a big step forward. The issue is addressed in Directive 2002/58/EC of 12 July 2002, above n. 2.

of the internet. The various data protection systems currently in place are extremely disparate. There may even be no protection at all in some countries through which data travels or on whose sites they end up. Another concern is raised by the case of Echelon, an integrated global surveillance network used to intercept messages transmitted by satellite owned by certain state information services including the United States, United Kingdom, Canada, Australia and New Zealand.[16] The idea that messages, including those in the national interest, can be captured by foreign powers as they are being transmitted by satellite demonstrates the limits of national sovereignty and the relative failure of national privacy protection systems. This is a particular problem in Europe.

Add to these features the opaque nature of the internet. The recent literature shows the range of applications said to have been engendered by means of cookies,[17] by the so-called 'global unique identifiers',[18] and through invisible hyperlinks.[19] This hidden face of the internet allows for picking and choosing between internet users. For instance, it facilitates various techniques of cyber-marketing, the efficacy of which becomes more remarkable by the day. These techniques permit such things as targeted advertising, differential pricing, even selective denial of access to websites by users deemed insufficiently financially worthwhile. The opaque nature of the internet further allows for the multiplication of actors, at times making it hard to identify readily their location, intervention or relationship between one another. Who knows about the precise role of internet access providers, of gateways and the link between these and the sites they list or refer to? Who knows about the role of search engines, not to mention browsers that pass on information to not easily identifiable actors, often without the knowledge of the users?

It follows that the internet entails major serious risks for the privacy of its users. This realisation forces a reconsideration of legislative provisions

[16] See European Parliament, *Report*, above n. 4.

[17] Cookies are pieces of information generated by a web server and stored in the user's computer when a web site is accessed. They allow web servers to recognise the user each time the site is returned to. In most cases, not only does the storage of personal information into a cookie go unnoticed, so does access to it: see, generally, Viktor Mayer-Schönberger, 'The Internet and Privacy Legislation: Cookies for a Treat?' (1997) 1 *West Virginia Journal of Law and Technology* 1.1.

[18] On this system developed by Microsoft, as well as on PSN (Personal Serial Number) developed by Intel, see J. Marc Dinant, 'Law and Technology Convergence in the Data Protection Field' in Ian Walden and Julia Hörnle (eds.), *E-Commerce Law and Practice in Europe* (Cambridge: Woodhead, 2002), chap. 8.2.

[19] See, in particular, J. Marc Dinant, *Les traitements invisibles sur Internet*, available at http://www.droit.fundp.ac.be/crid.

and the principles upon which these are based. That will be the focus of the next discussion. The adoption of new rights will be addressed under a separate heading. The chapter will end with a look at how the market itself may provide more effective privacy protection.

Towards a reconsideration of the legal rules and principles on privacy protection

The invasion of everyday life by the internet is a recent phenomenon. The European Directives and their national implementation measures could not take into account this development and its associated risks. In determining how the principles and concepts of the Directives on privacy protection will be applied, we first need to interpret the existing rules. Only where the existing law fails to provide a satisfactory solution is it necessary to resort to more proactive methods of rule creation. A comprehensive examination of the privacy Directives is beyond the scope of this chapter. The discussion below is limited to analysing certain relevant legislative provisions, reflecting on the conditions for legitimate use (in particular the notion of consent), and ending with some consideration of cross-border flows of information.

Definition of 'personal data'

One of the more controversial issues is the extension of the concept of personal data to information created by cookies. Recent literature on this issue starts from the proposition that cookies put information onto the hard drive of the user's computer so as to allow identification, not of the user personally but of his or her computer.[20] Each time the user reconnects to the relevant site, recognition occurs. According to Article 2(a) of the 1995 Data Protection Directive, personal data is 'any information relating to an identified or identifiable natural person' (the 'data subject'). Does this mean that information collated by cookies is beyond the scope of the privacy protection laws simply because only a computer is being identified? The 1995 Directive treats as identifiable a person who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to his or her physical, physiological,

[0] See, in particular, Marie-Hélène Boulanger and Cécile de Terwangne, 'Internet et le respect de la vie privée' in *L'Internet Face au Droit* (no. 12, Namur: Centre de Recherche Informatique et Droit, 1997).

mental, economic, cultural or social identity. Pursuant to preamble 26 of the 1995 Directive, for the purpose of determining the notion of 'identifiability' the totality of the means 'likely reasonably to be used', either by the controller or by any other person, should be taken into account. Does this assessment occur *in abstracto* or *in concreto*? The terms of the Directive do not answer this question. Yet, it is a relevant question because companies working with cookies generally claim that they do not engage in research to identify the physical person.

This concept of 'identity' applied to cookies but applying it beyond – to a global unique identifier or a simple IP address[21] – remains ambiguous. And this ambiguity remains in the way it was interpreted by various European countries when they transposed the 1995 Directive into their respective national legislation. I shall take as examples the transpositions carried out by Belgium, the United Kingdom and Sweden.

Belgian law defines as personal data:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[22]

This is a carbon copy of the text of the directive.

The scope of the British legislation is narrow because it states that:

> personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.[23]

The Freudian slip may be noted. It could be said that data relating to an individual are not personal data if the data controller cannot identify the person concerned. However, in this situation there are no personal data,

[21] Or, as regards the future IPv6, see Article 29 Working Party, *Opinion 2/2002 on the use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of IPv6*, 10750/02/EN/final, WP 58, 30 May 2002.

[22] Law of 8 December 1992, as modified by the Law of 11 December 1998. A consolidated version of this law is available at the web site of the Belgian Privacy Commission (which can also be translated as the Data Protection Authority or the Commission for the Protection of Personal Privacy), http://www.privacy.fgov.be.

[23] Data Protection Act 1998, s. 1. As regards the narrow interpretation of the concept under case law, see *Durant* v. *Financial Services Authority* [2004] FSR 28.

there is no processing of data and, consequently, there could be no 'data controller'.[24]

In Sweden, the Personal Data Act 1998 defines personal data as '(a)ll kinds of information that directly or indirectly may be referable to a natural person who is alive'. Surprisingly, no mention is made here of the notion of identity.[25] It could be thought that the Swedish law (which was intended to transpose the 1995 Directive) considers that information cannot be attributed to a natural living person without him or her being identified. On the internet, it is possible to imagine a customer who cannot be identified at all (for example, by using an anonymising site) and is assigned a number of non-identifying cookies attesting to his or her homosexuality and interest in AIDS treatments. In the strict framework of the 1995 Directive, the law would not apply to these two cookies because they do not relate to an identifiable person. However, the website (for example, one offering life assurance quotations online) that receives this visitor and his or her cookies could conclude, rightly or wrongly, that he or she has a relationship with a homosexual who probably has AIDS. The Swedish law, on the other hand, could become applicable if the feature 'homosexual, probably with AIDS' is *attributable*, at the moment of the connection, to a living natural person, even if he or she remains unidentifiable.

Saying that, we have to concede that considering an item of data (such as a cookie, the IP address or a global unique identifier) as 'personal data' will lead to the application of the provisions of the 1995 Data Protection

[24] Here, the drafters have disregarded the precision introduced by Recital 26 of Directive 95/46/EC of 24 October 1995, above n. 1. This leads to collateral damage: imagine the manager of a supermarket simply noting the registration numbers and types of the vehicles in the car park as well as their arrival and departure dates and times. Generally, it is not very likely that a supermarket manager will be able to go so far as to identify the person concerned simply from the registration number in his or her possession. This type of recording system would therefore not be covered by the UK's Data Protection Act 1998. There are no personal data, so there is no data processing let alone a 'data controller'. This system can be extended, refined and consolidated at the national level and this would provide a system that enables vehicles to be tracked via the car parks throughout the country. It is thus easy to imagine such a system on the internet in a data paradise, with anyone whatsoever being able to piece together the itinerary or even timetable of his or her neighbour, boss, lover or spouse.

[25] On this ambiguous concept applied to the genetic data, see Gaia Bernstein, 'Information Technologies and Identity' [2005] 1 *Computer Law Review International* (formerly *Computer und Recht International*) 1–7.

Directive 95/46/EC and, accordingly, the obligation to process this data,[26] even though it would not normally have been processed. In addition, the application of the provisions, such as the obligation to inform the person concerned, could prove impossible without identifying him or her. But in another sense, we have to underline that not treating the IP address and the global unique identifier as items of personal data would pose a problem because of the risks that subsequent use of these data represent in terms of profiling the individual and, indeed, the possibility of contacting him or her. There is evidence that, with the combination of web traffic surveillance tools, it is easy to identify the behaviour of a machine and, behind the machine, that of its user. In this way the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the 'identity' of the individual – that is, his or her name and address – it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her identity in a traditional sense.

Categories of data

The scope of application of the Privacy and Electronic Communications Directive 2002 is considerably wider than the 1997 Directive it replaces. Whereas the 1997 Directive applied to telecommunications services and networks, the 2002 Directive covers all services and networks in the electronic communication sector, at least where these are open to the general public. The idea is to bring within the same regulatory framework all services and networks whose main object is the transmission and routing of signals regardless of the technology used, including provision of access to the internet as well as 'remailing' services. This extended coverage of European law is important in that it sets up a separate regime for data processing that occurs within these networks, in particular involving data about traffic and so-called location data. The latter is a new concept. The former already featured in the 1997 Directive, but the 2002 Directive now provides a definition of both concepts.

[26] If only to enable rights of access, and so forth.

Under the 2002 Directive, the concept of traffic data embodies 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[27] This includes the address label of an internet transmission – either that of the sender or the receiver – the length of the communication and also the protocols used. Pursuant to Article 6 of the 2002 Directive, this type of data must be 'erased or made anonymous when it is no longer needed for the purpose of the transmission of the communication'. Three exceptions are allowed: where the data is needed for billing purposes; where consent, which might be revoked at any moment, is given for the purpose of marketing electronic communication services or the provision of value added services; and where the data is required by proper authorities for settling disputes, in particular about interconnection or billing.[28]

Location data are defined as 'any data processed in an electronic telecommunications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.[29] Examples are precision location data attached to the possession and use of mobile terminal equipment, the offer of value added services by some operators, and services that rely on localisation being possible such as, for example, guidance services for drivers. The 2002 Directive prohibits the processing of the above data without the revocable consent of the user or subscriber to the service, or beyond the extent or duration necessary for such service.[30] Users or subscribers must be given the possibility to withdraw their consent at any time.

An analysis of the European provisions on traffic and location data reveals important deviations from the principles on the legitimacy of data processing as signalled by Article 6 of the 1995 Data Protection Directive. Under the 1995 Directive interests may be weighed in deciding whether data processing is permitted.[31] Under the 2002 Directive, the primary if not sole basis for the processing of traffic and location data is when it is duly legitimated by the service offered or the prior consent of the persons

[27] Directive 2002/58/EC of 12 July 2002, above n. 2, Art. 2(b). On the European regulation of traffic data, see Brigitte Zammit, 'Traffic Data Retention under EC Law' (2005) 11(1) *Computer and Telecommunications Law Review* 17.

[28] Directive 2002/58/EC of 12 July 2002, above n. 2, Art. 6(b) and (c).

[29] Ibid. Art. 2(c).

[30] Ibid. Art. 9(b).

[31] Directive 95/46/EC of 24 October 1995, above n. 1, Art. 7(f), discussed below n. 36 and accompanying text.

concerned.[32] This restriction, when applied in the context of internet use, can be striking.[33]

Legitimacy of the processing

Consent as a basis for the legitimacy of processing

The scope for applying the consent requirement in the context of the internet is extremely wide. For instance, it makes employer monitoring of employee internet use, including the transfer from site to site via hyperlinks, conditional upon the user's consent.[34] Two justifications for this omnipresent consent requirement come to mind.[35] The first has to do with the risks associated with the possible multitude of processing operations. It justifies adopting a restrictive approach to the grounds for legitimate data processing. In particular, it calls for close scrutiny of

[32] Traffic data retention for law enforcement purposes or for the network's own security purposes is not developed. On that point, see the discussion around the presently discussed *Draft Framework Decision on the Retention of Data*, above n. 7. On the draft, EPIC comments and further material are available at http://www.epic.org./privacy/intl/data_retention.html.

[33] Thus, e.g., Art. 314, 2 of the Belgian Penal Code prohibits anyone from receiving, intercepting, or listening to private communications or telecommunications, unless all parties concerned agree. The 17th Chamber of the Criminal Court of Paris had occasion to enforce this principle when it ruled against a research laboratory that expelled a student upon becoming aware of personal email use: Corr Paris, 2 November 2000. The text of the decision can be found at http://www.droit-technologie.org.

[34] The Belgian Privacy Commission has issued a qualified recommendation in this regard: Commission de la Protection de la Vie Privée, *Avis no. 10/2000 d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail*, 3 April 2000. Recommendation 10/2000 acknowledges a certain legitimacy of employer control over the use of company equipment. For the Commission the question is one of proportionality between the control mechanisms used and the risks run by the employer. Thus, checking the contents of employee email is not necessarily legitimate where the installation of filters can equally reduce illegitimate use. As regards the German situation, the same principles are available; see, on that point, Jan-Malte Niemann, 'Monitoring Internet and Email Usage – Germany – Surfing into Unemployment? Private Internet Use and Emailing Under German Labour Law' (2002) 18(2) *Computer Law and Security Report* 114. It would seem that in North America employees do not enjoy a similar 'reasonable expectation' that their privacy is to be protected in the use of the email system: see, H. L. Rasky, 'Can an Employer search the Contents of his Employees' E-mail?' (1998) 20 *Advocates' Quarterly* 221.

[35] On the consent requirement we might take into account the warnings by Léonard against an overly wide application; see Thierry Léonard, 'E-commerce et protection des données à caractère personnel: quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet', February 2000, available at http://www.droit.fundp.ac.be/Textes/Leonard1.pdf.

Article 7(f) of the 1995 Directive as that provision permits data processing following a weighing of the various interests at stake.[36] This weighing of interests is difficult to carry out in practice. It presupposes that the individual concerned is able to know all the processed data and able to ensure that his or her interests are taken into account. At times this can be most problematic given the global nature of the network. The second justification relates to the interactive nature of the network, in that this allows for consent to be fully possible. In effect, it is the person concerned who, by using his or her equipment, is the author of the data created. Why not let that person decide whether he or she wishes to receive cookies, identify himself or herself, have his or her data transmitted to a third party, receive advertising messages, and so forth? Consent allows the consumer to decide whether or not he or she wishes to part, possibly in exchange for hard currency, with his or her personal data.

The requirement that there be a legitimate purpose involves considering the question of consent as the basis for the legitimacy of certain processing operations carried out in connection with the use of internet services by the data subject. As we know, even if Article 5 limits itself to mentioning the general principle of legitimacy, the issue of consent is mentioned by the data protection authorities, by the European Directive in Article 5.1, and by legal writers as the primary basis for the legitimacy of a processing operation. Since modern networks are interactive, consent can more easily be claimed to be the basis for the legitimacy of data processing and be preferred to other more traditional bases such as a balance of interests. The ease with which the file controller can obtain the data subject's consent explains why some countries' laws do not hesitate now to demand that consent be given in order to legitimise certain processing operations, like the 2002 Directive on the processing of traffic and location data.[37]

This consideration now leads some to believe that consent may be enough to legitimise processing. It should be remembered in this connection that the development by the World Wide Web Consortium (W3C) of

[36] Directive 95/46/EC of 24 October 1995, above n. 1, Art. 7(f) provides that data processing may be permitted if 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which requires protection under Article 1(1)'.

[37] Mention should also be made of the opt-in system chosen to resolve the question of sending unsolicited mail. Other arguments in favour of the ability to opt in are the intrusive character of the mail that directly penetrates the data subject's home, the ease with which such messages can be sent and the absence of any costs for the sender.

the Platform for Privacy Preferences (P3P)[38] was also based on the possibility for web surfers to negotiate with service providers who failed to respond to their privacy preferences and reach an agreement that would serve as a legitimate basis for the planned processing operation. Even if no broad use has ever been made of this possibility of holding negotiations, especially through electronic agents, P3P remains an indication of the industry's willingness to provide itself with the means of negotiating with the data subject the use that might be made of his or her data. The protection of privacy could thus to some extent be negotiated.[39]

Nevertheless consent does not appear to us to be a sufficient basis for legitimacy. We think that, in certain cases, even the legitimacy of processing that is backed by a person's specific, informed and freely given consent may be called into question. There are three reasons that support this view. First, even consent that has been obtained by fair means cannot legitimise certain processing that is contrary to human dignity or to other key values that an individual cannot relinquish. Secondly, consumers must be protected against practices that involve their consent being solicited in exchange for economic advantages.[40] Finally, the question of the protection of privacy is not just a private matter, but brings social considerations into play and calls for the possibility of intervention and supervision by authorities.[41]

The consent of minors to the processing of personal data concerning them poses some tricky problems. The consent must come from a person legally capable of giving it. The consent given by a minor is on no account sufficient without parental authorisation, but this does not prevent minors having to be consulted – provided that they understand – or even requiring not only parental authorisation but also the minor's own autonomously

[38] See Article 29 Working Party, *Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, XV D/5032/98, WP 11, 16 June 1998. See also, on this protocol, Jason Catlett, *Open Letter 9/13 to P3P Developers*, 13 September 1999, available at http://www.junkbusters.com/standards.html.

[39] On the technology-based contractualisation of the processing of data, see Paul M. Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace, Filters, Privacy Control and Fair Information Practices' (2000) *Wisconsin Law Review* 749; Marc Rotenberg, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' (2001) *Stanford Technology Law Review* 1.

[40] As noted by Léonard, 'E-commerce et protection', above n. 35, the rules in general contract theory as regards defects in the consent, especially the rules on taking unfair advantage, must be complied with.

[41] Cf. in this connection the thoughts put forward by Schwartz, 'Beyond Lessig's Code for Internet Privacy', above n. 39.

expressed consent. Recently, the development of interactive internet services has given these principles a particular topicality. Children are a preferred target for all kinds of internet 'vendors' and several methods of gathering information are used to induce them to provide personal information, such as competitions, membership forms, and so forth. It thus appears necessary to check parental consent to the provision of such information. The US Children's Online Privacy Protection Act (COPPA) of 1998 requires that the provider of services that gather information from minors be subject to the principle of 'verifiable parental consent', which is defined as:

> any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.[42]

Recently, the Belgian Privacy Commission issued a more guarded opinion on the same subject, stressing the child's autonomy and underlining the limits to it:

> The Commission is of the opinion that parental consent does not have to be systematically required when data relating to a minor are processed on the internet. It thus emphasises that parental consent should not be a mechanism permitting a parent to override the child's decision unless there is a serious risk that the child will not correctly appreciate the consequences of its decision or that its natural naivety will be exploited. The Commission therefore stresses in this document the necessity to obtain parental consent in specific circumstances, especially when the child has not reached the age of discernment, when sensitive data are gathered, when the aim pursued is not in the minor's direct interests (marketing, transmission of the data to third parties) or when the data are to be made public (dissemination of information at a discussion forum or at a school's website).[43]

[42] Children's Online Privacy Protection Act 1998 (US) s. 1302(9). The text of the law is available at the Federal Trade Commission's website http://www.ftc.gov/ogc/coppa1.htm. The law provides for some exceptions to this requirement.

[43] Belgian Privacy Commission, *Opinion on the Protection of the Privacy of Minors on the Internet*, Avis no. 38/2002, 16 September 2002. Available at the Commission's website: http://www.privacy.fgov.be.

Incompatible processing

The principle of the 'compatibility' of purposes requires that, in the case of subsequent processing, these operations must not clash with the reasonable expectations of the person concerned. The acceleration of technological progress, the infinite number of new processing opportunities offered by the software, and the data available on the network warrant giving some attention to the question of subsequent processing and its compatibility with the initial aims of data recording. More and more data are stored in huge data warehouses in order to be reused in the future for new applications, taking into account new technological possibilities or scientific progress.

For example, Radio Frequency Identifier or RFID chips, which were originally designed by consumer goods manufacturers as a means of preventing theft in big department stores, have become a powerful tool for analysing the behaviour of consumers, their profiles, and so forth. If scientific authors make their curriculum vitae and publications available for the purpose of making their work known, this may serve to classify them politically or in terms of their analyses. The publication of court judgments in huge databases has an academic objective and helps to make the law known. However, the possibility of running a search of the names of the parties or the type of case may enable blacklists to be drawn up (for example, a list of employees who have brought an action against or been dismissed by their employers).

The proportionality of the data

Some comments about the contents of data processing are in order. The European Directive asserts clearly that the data processed must be relevant, proportionate and not excessive as regards the legitimate purposes pursued by the data controller. The possibilities offered by the internet in collecting data, especially given the interactive nature of the net, explain the discrepancy between the sheer volume of data retained or handled and the legitimate purpose pursued by those responsible for processing the data. An example is the data processing that occurs in the context of employee surveillance by companies.[44] An illustration may be given from

[44] Pursuant to this principle, what the Belgian Privacy Commission questions is not so much the legitimacy of the data handling but rather the possible disproportionate size of their contents. To control an employee's activities does not necessitate the detailed collection of all terminal activity by that employee. Rather, the collection of general data may suffice such as, e.g., time spent on the computer, type of services used. See, on the opinion of the Belgian Privacy Commission, Stanislas Van Wassenhove, Michael De Leersnyder and Gael Chuffart, *Nouvelles technologies et impact sur le droit du travail* (Kortrijk-Heule: UGA, 2003) pp. 81–97.

a 1998 OECD study on electronic commerce sites.[45] The study shows that for nearly two thirds of sites the information asked for – via subscription lists, feedback forms, and especially questionnaires – is optional. Among this optional information typically feature the individual's email address, telephone number, age, gender, occupation, certain preferences and personal habits. At times the answers to these optional questions allowed visitors to gain award points or enter a competition.

Trans-border data flows

The internet and over 60 percent of sites continue to be North American: any European traffic on the internet takes place on non-European webs. This explains the concern of the public authorities about cross-border movement of data. The provisions of Articles 25ff of the 1995 Directive hold that the transfer to a non-EU country of personal data that is the object of processing after their transfer cannot occur unless the country in question provides assurance about an adequate level of data protection. Exceptions to this principle exist, either in certain specific instances of legitimate movement, or where sufficient contractual safeguards are in place. Without claiming to be exhaustive, two questions arise. A first question concerns the scope of application of the provisions. A second question concerns the standards adopted by foreign countries for the provision of adequate data protection safeguards.

As to the first, Article 4 of the 1995 Directive provides that Member States should apply their laws extraterritorially where 'for the purposes of processing personal data [the controller] makes use of equipment . . . situated on the territory of the said Member State, unless the equipment is used only for purposes of transit through the territory of the Community'. Many academic scholars concur with Boulanger and Terwangne who argue that the Directive applies to narrowly defined instances of passive trans-border movements; that is, those that occur without the knowledge of the person concerned and that involve the use from a distance

[45] OCDE, *Pratiques relatives à la mise en oeuvre sur les réseaux mondiaux des lignes directrices de l'OCDE sur la vie privée*, DSTI/ICC/REG (98) 6, Paris, 18 and 19 May 1998.

of the user's equipment to collect data.[46] Also covered is data processed by cookies or other means such as the global unique identifier as well as cases of 'web spoofing' where data collection occurs via a mirror site based in a European country.[47] An analogous case is the case of Yahoo which gained some adverse publicity when proceedings were launched by *La Ligue Contre le Racisme et l' Antisémitisme* objecting that anti-Semitic material could be accessed from one of its websites. It was shown that the site Yahoo.fr simply served as a collection instrument without local handling of the data in France. The French court ruled against the Yahoo company.[48]

Some commentators have raised doubts about the applicability of Articles 25ff of the 1995 Directive whenever the user is in direct contact with a foreign site. Modifications have been made in some of the implementing national laws. For instance, Article 3bis of the Belgian law limits its reach to instances where the processing occurs in the context of real and effective activities of a business based in Belgium or where the processing is done by means, whether or not automated, in Belgium. The first scenario is said not to cover instances where the data generated by a site visit do not constitute handling or processing, at least not in Europe. However, this interpretation seems to go against the 1995 Directive, which the Belgian legislation was meant to implement. The Directive gives the Member States specific powers in matters of trans-border movements, whether or not the exported data have been the subject of processing in Europe. And Article 4 of the 1995 Directive, upon which Article 3bis of the Belgian legislation is based, does not seek to determine the substantive scope of application of the Directive; rather it sets out to determine the applicable national law as regards data processing.

[46] Marie-Hélène Boulanger and Cécile de Terwangne, 'Internet et le respect de la vie privée' in Etienne Montero (ed.), *L'internet face au droit*, Cahier du CRID no. 12 (Namur: Story-Scientia, 1997).

[47] In that sense, see Article 29 Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Websites*, 5035/01/EN/Final, WP 56, 30 May 2002.

[48] The case concerned the complaint by several French groups against the Yahoo company for harbouring Nazi objects on its sites. The president of the French court of first instance at two occasions (on 22 May and again on 20 November 2000) ordered Yahoo to take all necessary steps to discourage and prevent the auctioning and sale of Nazi memorabilia. The text of the decisions of the Tribunal de Grande Instance, as well as some commentaries, is available at www.juriscom.net/txt/jurisfr/cti/ tgiparis20001120.htm. For parallel action taken in the United States by Yahoo, see *Yahoo!, Inc.* v. *La Ligue Contre Le Racisme et L'Antisémitisme*, 379 F 3d 1120 (9th Cir. 2004) and 399 F 3d 1010 (9th Cir. 2005).

In the *Lindqvist* case,[49] the European Court of Justice had to solve the following question. Does the insertion on a web page located on a host server located in Europe but accessible from foreign countries constitute a trans-border data flow in the sense of Articles 25ff? In a highly criticised decision,[50] the court considered that the author of the website pages containing personal data had not transferred the data to foreign countries insofar as the author only furnished the pages to a national hosting provider, even if the purpose was to render these web pages accessible throughout the world. The main reason invoked by the court was its concern of seeing all postings on internet web pages automatically subject to the restrictions imposed by Articles 25ff.

If it is correct that Articles 25ff of the 1995 Directive apply to most trans-border movements via the internet, a determination of the adequate nature of the safeguards offered by the foreign country must be made. The EC Commission examined the Safe Harbour Principles drafted by the US Department of Commerce, to which American companies are expected to subscribe,[51] and concluded that they satisfy the adequate safeguard requirement of the Directive – although this has not been the case for all countries whose privacy laws have been reviewed by the Commission.[52] Furthermore the European Commission has proposed to companies alternative models offering 'appropriate safeguards' for the transfer

[49] *Lindqvist* [2003] ECR I-12971; [2004] QB 1014 (Case C-101/01).

[50] See, in particular, Cécile de Terwangne, 'Affaire *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles' (2004) 19 *Revue du Droit des Technologies de l'Information* 67 at 88ff.

[51] The text of the safe harbour principles may be found on the internet site of the US Department of Commerce at http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm. In brief, six basic principles form the core of the 'Safe Harbor Principles'. They relate to information on the person concerned; restrictions on transfer; security; integrity of the data; access by the person concerned and effectiveness of the principles themselves. As for the latter, there exist mechanisms to appeal to independent private authorities and action may be taken by the Federal Trade Commission in instances of misrepresentation. On the implementation of the Safe Harbour Principles and its assessment, see the CRID study prepared for the EU Commission (Internal Market DG): Jan Dhont, María Verónica Pérez-Asinari and Yves Poullet (with the assistance of Joel R. Reidenberg and Lee A. Bygrave), *Safe Harbour Implementation Study* (Namur: CRID, 2004); available from http://europa.eu.int/comm/justice_home/fsj/privacy/.

[52] Other decisions have been taken by the Commission under the Article 25.6 basis, notably vis-à-vis Argentina, Switzerland, Canada. The legislative system proposed by Australia as regards the private sector on the contrary has been judged as inadequate by the Commission insofar as notably too broad exceptions have been allowed under the Australian Act for small enterprises, employees' data and the absence of protection for foreigners' data (See: Article 29 Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN, WP 40, 26 January 2001).

of personal data.[53] So the Commission adopted in 2001 two decisions on standard contractual clauses for the transfer of the data outside the European Economic area – for the transfer of personal data to controllers and processors established abroad[54] – and more recently has issued an opinion about 'binding corporate rules'; that is, self-regulatory data protection safeguards which are put in place by multinational companies on the basis of their own needs and culture and offer more flexibility than contractual clauses.[55]

Towards the recognition of new rights

Those features that are most characteristic of the electronic communications service environment – growing presence and multifunctionality of electronic communications networks and terminals, their interactivity, the international character of networks, services and equipment producers and the absence of transparency in terminal and network functioning – all increase the risk of infringing individual liberties and human dignity.

To counter these risks, certain new principles must be established if data subjects are to be better protected and have more control over their environment. Such control is essential if those concerned are to exercise effective responsibility for their own protection and be better equipped to exercise proper informational self-determination. This is a first attempt to outline such principles. It is based on a range of material and we have tried to structure it around five main principles, since at this stage we prefer not to speak of new 'rights' for data subjects. Their content and extension should be discussed by the Council of Europe Consultative Committee on Convention no. 108, and could then, if appropriate, form the basis for recommendations and other ad hoc measures to give them greater force.

[53] The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26(4) of Directive 95/46/EC that certain standard contractual clauses offer sufficient safeguards as required by Article 26(2), that is, they provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

[54] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document no. C(2001) 1539) 2001, *OJ*, L 181, 4 July 2001, 19; and Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (notified under document no. C(2001) 4540) 2002, *OJ*, L 006, 10 January 2002, 52.

[55] Article 29 Working Party, *Working Document on Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, MARKT/11639/02/EN, WP 74, 3 June 2003.

The principle of encryption and reversible anonymity

The encryption of messages offers protection against access to the content of communications. The quality varies, as do encryption and de-encryption techniques. Encryption software for installation on internet users' computers (S/MIME or Open PGP protocols) is now available at a reasonable price. Given its ambiguity, the notion of anonymity should perhaps be clarified, and possibly replaced by other terms such as 'pseudonymity' or 'non-identifiability'. What is sought is often not absolute anonymity but rather the functional non-identifiability of the author of a message vis-à-vis certain persons.[56] There are many non-binding documents advocating citizens' 'right' to anonymity when using new technological services.[57] Recommendation R (99) 5 of the Council of Europe's Committee of Ministers states that 'anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy',[58] hence the importance of privacy enhancing techniques already available on the market.

Those using modern communication techniques must be able to remain unidentifiable by service providers and other third parties during the transmission of the message and by the recipient or recipients of the message, and should have free or reasonably priced access to the means of exercising this option.[59] The availability of readily affordable encryption and anonymisation tools and services is a necessary condition for computer users exercising personal responsibility.

[56] See Jan Grijpink and Corien Prins, 'Digital Anonymity on the Internet: New Rules for Anonymous Electronic Transactions?' (2001) 17 *Computer Law and Security Report* 379.

[57] See, in particular, Stefano Rodota, 'Beyond the EU Directive: Directions for the Future' in Yves Poullet, Cécile de Terwangne and Paul Turner (eds.), *Privacy: New Risks and Opportunities*, Cahier du CRID no. 13 (Antwerpen: Kluwer, 1997) p. 211ff.

[58] Council of Europe, Committee of Ministers, *Guidelines for the Protection of Individuals with regard to the Collection and Processing of Personal Data on Information Highways*, Recommendation no. R (99) 5, 23 February 1999. See also Article 29 Working Party, *Recommendation 3/97: Anonymity on the Internet*, DG MARKT D/5022/97, WP 6, 3 December 1997; and the opinion of the Belgian Privacy Commission on electronic commerce: *Avis no. 34/2000 relatif à la protection de la vie privée dans le cadre du commerce électronique*, 22 November 2000 (available at http://www.privacy.fgov.be) which points out that there are ways of authenticating the senders of messages without necessarily requiring them to identify themselves.

[59] See the recommendation of the French Commission for Privacy that access to commercial sites should always be possible without prior identification: Marie Georges, 'Relevons les défis de la protection des données à caractère personnel: l'Internet et la CNIL' in P. Lemoire (ed.), *Commerce électronique- Marketing et vie privée* (Paris: LaSer, 1999), pp. 71–2.

The anonymity or 'functional non-identifiability' required, however, is not absolute. Citizens' right to anonymity has to be set against the higher interests of the state, which may impose restrictions if these are necessary 'to safeguard national security, defence, public security, [and for] the prevention, investigation, detection and prosecution of criminal offences'.[60] Striking a balance between the legitimate monitoring of offences and data protection may be possible through the use of 'pseudo identities', which are allocated to individuals by specialist service providers who may be required to reveal a user's real identity, but only in circumstances and following procedures clearly laid down in law.

Other approaches might include the enforced regulation of terminal equipment, to prevent browser chattering, permit the creation of ephemeral addresses and differentiation of address data according to which third parties will have access to the traffic or localisation data, and the disappearance of global unique identifiers by the introduction of uniform address protocols.

Finally, the status of 'anonymisers', on which those who use them place great reliance, should be regulated to offer those concerned certain safeguards regarding the standard of service they provide while ensuring that the state retains the technical means of accessing telecommunications in legally defined circumstances.[61]

The principle of reciprocal benefits

This principle would make it a statutory obligation, wherever possible, for those who use new technologies to develop their professional activities to accept certain additional requirements to re-establish the traditional balance between the parties concerned. The justification is simple – if technology increases the capacity to accumulate, process and communicate information on others and facilitates transactions and administrative operations, it is essential that it should also be configured and used to ensure that data subjects, whether as citizens or consumers, enjoy a proportionate benefit from these advances.

Several recent provisions have drawn on the proportionality requirement to oblige those who use technologies to make them available for users

[60] Directive 2002/58/EC of 12 July 2002, above n. 2, Art. 15.

[61] Requirements could be laid down for the services provided and concerning confidentiality, as is proposed for electronic signatures. Official approval of an anonymiser would indicate that the requirements were being observed. Such official approval might be voluntary rather than obligatory, as in the case of quality labels.

to enforce their interests and rights. So Article 5.3 of the 2002 Directive on privacy and electronic communications even includes the requirement that 'the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information . . . and is offered the right to refuse such processing'. Subscribers' right, under Article 8.1, 'via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis . . . and on a per-line basis' is another potentially valuable approach if the notion of 'calling line' is extended to various internet applications, such as web services and email.[62] This implies a related obligation for the service provider to offer users the options of refusing to accept unidentified calls or preventing their identification.[63]

Legislation of the freedom of information variety introduces a similar right to transparency vis-à-vis government by adding further information that the latter is obliged to supply. A welcome development in the UK is the recent introduction of a public service guarantee for data handling.[64] A Swedish commission has recently recommended legislation that would entitle citizens to monitor their cases electronically from start to finish, including their archiving, and oblige the authorities to adopt a good public access structure, to make it easier for individuals to identify and locate specific documents.[65] There is even draft legislation that would make it possible to link any official documents on which decisions were based to other documents about the case. In other words, a public service that has become more efficient thanks to new technology must also be more transparent and accessible to citizens. Citizens' right of access extends beyond the documents directly concerning them to include the regulations on which a decision was based.

[62] Note the link between these provisions and the anonymity principle.

[63] See Art. 8.2 and 8.3 of Directive 2002/58/EC of 12 July 2002, above n. 2.

[64] The UK Department for Constitutional Affairs has released a public service guarantee for data handling which is available for implementation in public bodies. It sets out people's rights about how their personal data is handled by public authorities and the standards they can expect public organisations to adhere to, see http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2.

[65] Peter Seipel, 'Information System Quality as a Legal Concern' in Urs Gasser (ed.), *Information Quality Regulation: Foundations, Perspectives, Applications* (Baden-Baden: Nomos, 2004) p. 248. See also the Swedish ICT Commission report: Peter Seipel (ed.), *Law and Information Technology: Swedish Views*, Swedish Government Official Reports, SOU 2002: 112.

It is even possible to imagine that certain of the rights associated with data protection – such as the right to information, the rights of access and rectification, and the right of appeal – might soon be enforceable electronically. Many applications could be proposed, including the five suggestions that follow.

It should be possible to apply data subjects' right to information at any time through a simple click (or more generally a simple electronic and immediate action) offering access to a privacy policy, which should be as detailed and complete as the greatly reduced cost of electronic dissemination allows. Such a step must be anonymous as far as the page server is concerned, to avoid any risk of creating files on 'privacy concerned users'. In addition, in the case of sites that have been awarded quality labels, it should be obligatory to provide a hyperlink from the label symbol to the site of the body that awarded the label. The same would apply for a declaration by a file controller to a supervisory authority: a hyperlink would be installed between any site processing personal data and that of the relevant supervisory authority. Finally, consideration might be given to the automatic signalling of any site located in a country offering inadequate protection.

In the future, data subjects must be able to exercise their right of access using an electronic signature. It would be obligatory to structure files so that the right of access was easy to exercise. Additional information, such as the origin of documents and a list of third parties to whom certain data had been supplied, should be systematically available. As noted earlier, increasingly, the personal data accumulated by the vast public and private networks are no longer collected for one or more clearly defined purposes but are stored in the network for future uses that only emerge as new processing opportunities or previously unidentified needs arise. In such circumstances, data subjects must have access to documentation describing the data flows within the network, the data concerned and the various users – a sort of data registry.[66]

It should be possible to exercise online the rights of rectification and/or challenge to an authority with a clearly defined status responsible for considering or maintaining a list of complaints. And the right of appeal

[66] This idea is the subject of two Belgian laws that require the establishment of sectoral committees for networks linked to the National Register (Act of 8 August 1983 establishing a national register of persons, as amended by the Act of 25 March 2003, MB. 28 March 2003, Art.12§1) and to the commercial registration authority (Banque Carrefour des entreprises) (Act of 16 January 2003 establishing the authority, MB. 5 February. 2003, Article 19§4).

should also benefit from the possibility of online referral, exchange of parties' submissions and other documentation, decisions and mediation proposals.

Finally, when individuals concerned wish to challenge decisions taken automatically or notified via a network (such as a refusal to grant a building permit following a so-called e-government procedure), they should be entitled to information, via the same channel, on the logic underlying the decision. For example, in the public sector citizens should have the right to test anonymously any decision-making packages or expert systems that might be used.[67] This might apply to software for the automatic calculation of taxes or of entitlement to grants for the rehabilitation of dwellings.

The principle of encouraging technological approaches compatible with or improving the situation of data subjects

Recommendation 1/99 of the EU Data Protection Working Party – the so-called Article 29 Working Party or Article 29 Working Group – is concerned with the threat to privacy posed by internet communications software and hardware.[68] It establishes the principle that software and hardware industry products should provide the necessary tools to comply with European data protection rules. In accordance with this third principle, regulators should be granted various powers.

For example, they should be able to intervene in response to technological developments presenting major risks. The so-called precautionary principle, which is well-established in environmental law, could also apply to data protection. The precautionary principle may require telecommunications terminal equipment (including software) to adopt the most protective parameters as the default option to ensure that those concerned are not exposed to various risks of which they are unaware and which they cannot assess. Similarly, in accordance with the principle of reciprocal benefits, it is appropriate and not unreasonable to equip telecommunications terminal equipment with log-in and log-out

[67] The same principle applies to private decision makers, subject to the legitimate interests of the file controller (particular relating to business confidentiality, which could limit the duty to clarify the underlying logic of the systems).

[68] Article 29 Working Party, *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*, DG MARKT 5093/98, WP 17, 23 February 1999.

data bases, as is the case with server-type software used by online businesses and government departments. This would enable users to monitor persons who have accessed their equipment and, where appropriate, identify the main characteristics of the information transferred.

This can be illustrated by one of the provisions of the 2002 Directive on privacy and electronic communications. Article 14 states that where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary, way of protecting personal data from the risks of unlawful processing – risks that have been created by all these new technological options. Going further, it is necessary to prohibit so-called privacy killing strategies,[69] in accordance with the security principle enshrined in Article 7 of Council of Europe Convention 108.[70] The obligation to introduce appropriate technical and organisational measures to counter threats to data privacy will require site managers: to make sure that messages exchanged remain confidential; to indicate clearly what data is being transmitted, whether automatically or by hyperlink, as is the case with cybermarketing companies; and to make it easy to block such transmission.

This security obligation will also require those who process personal data to opt for the most appropriate technology for minimising or reducing the threat to privacy. This requirement clearly has an influence on the design of smart cards, particularly multifunctional cards, such as identity cards.[71] Another example of the application of this principle concerns the structuring of medical files at various levels, as recommended by the Council of Europe.

It might be possible to go further by recommending the development of privacy enhancing technologies, that is tools or systems that take more account of data subjects' rights. Clearly, the development of these technologies will depend on the free play of the market but the state must play an active part in encouraging privacy compliant and privacy enhancing products by subsidising their research and development, establishing equivalent voluntary certification and accreditation

[69] The expression is used by Dinant, 'Law and Technology Convergence', above n. 18.

[70] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, opened for signature 28 January 1981.

[71] On the privacy compliant design of multi-application cards, see Ewout Keuleers and J. Marc Dinant, 'Data Protection: Multi-Application Smart Cards: The use of Global Unique Identifiers for Cross-Profiling Purposes – Part II: Towards a Privacy Enhancing Smart Card Engineering' (2004) 20(1) *Computer Law and Security Report* 22–8.

systems and publicising their quality labels, and ensuring that products considered necessary for data protection are available at affordable prices.[72]

Users' right to full control of terminal equipment

The justification for this principle is obvious. Since these terminals can enable others to monitor our actions and behaviour, or simply locate us, they must function transparently and under our control. Article 5.3 of the 2002 Directive, cited above,[73] offers a first illustration of this point. Those concerned must be informed of any remote access to their terminals, via cookies, spyware or whatever, and must be able to take easy and effective countermeasures, free of charge. The 2002 Directive also establishes the rule that users of calling and connected lines can prevent the presentation of the calling line identification.

Going beyond these examples, we would also argue that all terminal equipment should be configured to ensure that owners and users are fully informed of any data flows entering and leaving, so that they can then take any appropriate action. Similarly, as is already the case under some legislation, possession of a smart card should be accompanied by the possibility of read access to the data stored on the card.

User control also means that individuals can decide to deactivate their terminals at any time. This is important as far as RFIDs are concerned. Data subjects must be able to rely on third parties that vouch that such technical means of remote identification have been fully deactivated.[74]

Users may well apply this principle to firms that are not necessarily covered by traditional data protection rules because they are not responsible for data processing. Examples include suppliers of terminal equipment and many forms of browser software that can be incorporated into terminals to facilitate the reception, processing and transmission of electronic communications. The principle also applies to public and private standard setting bodies concerned with the configuration of such material and

[72] On co-regulatory developments, see Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (London: Ashgate, 2003); Yves Poullet, 'Making Data Subjects Aware of Their Rights and Capable of Protecting Themselves', Conference on the Rights and Responsibilities of Data Subjects, Council of Europe, Prague, 14–15 October 2004 (being published).

[73] See above n. 62 and accompanying text.

[74] Clearly this refers to accreditation arrangements such as those already described as joint regulation, above nn. 36–7 and accompanying text, or to approval issued by the authorities to certain undertakings (i.e. public regulation).

equipment. The key point is that the products supplied to users should not be configured in such a way that they can be used, whether by third parties or the producers themselves, for illicit purposes. This can be illustrated by a number of examples.

First, a comparison of browsers available on the market shows that chattering between them goes well beyond what is strictly necessary to establish communication.[75] Secondly, browsers differ greatly in how they receive, eliminate and prevent the sending of cookies, which means that the opportunities for inappropriate processing will also vary from one browser to another. However, blocking pop-up windows or the systematic communication of references to articles read online or of keywords entered in search engines is apparently impossible, at least in a simple way, on the default browsers installed on the majority of the hundreds of millions of personal computers. Finally, attention should also be drawn to the use of unique identifiers and spyware by suppliers of browser tools and communication software.

More generally, terminal equipment should function transparently so that users can have full control of data sent and received. For example, they should be able to establish, without fuss, the precise extent of chattering on their computers, what files have been received, their purpose and who sent or received them. From that standpoint, a data base automatically ensuring the registration of all entering and outgoing flows appears to be an appropriate tool that is relatively easy to introduce.

In addition to users' right to be informed of data flows, there is the question of whether persons are entitled to require third parties to secure authorisation to penetrate their 'virtual home'. Of relevance here is the Council of Europe Convention on Cybercrime,[76] particularly Article 2 concerning illegal access,[77] and Article 3 about illegal

[75] See J. Marc Dinant, 'Le visiteur visité – Quand les éditeurs de logiciel internet passent subrepticement à travers les mailles du filet juridique' (Winter 2001) 6:2 *Lex Electronica*, available from http://www.lex-electronica.org.

[76] Council of Europe, Convention on Cybercrime, CETS No. 185, opened for signature 23 November 2001.

[77] Article 2 – Illegal access:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

interception.[78] In this case, the identification or identifiability of persons taking part in telecommunications is not a precondition for the Convention's application. Similarly, unauthorised access to a computer system is not confined to hacking into major systems operated by banks or government departments but also concerns non-authorised access to telecommunications terminals, represented in the current state of the art by computers.[79]

In other words, we maintain that placing an identifying number in a telecommunications terminal (or simply accessing this number or some other terminal identifier) generally constitutes unauthorised access. In such a legal context, there can be no question of assessing the proportionality of such actions. Authorisation remains a positive act that is quite distinct from any acceptance that might be inferred from silence or a failure to object. It cannot therefore be assumed – as DoubleClick did[80] – that simply by failing to activate a cookie suppressor users have authorised all and sundry to install this type of information on their terminals.

Privacy, the internet and consumer rights

The routine use of information and communication technologies, formerly confined to major undertakings, and the rapid development of electronic commerce that has multiplied the number of online services have led to a more consumerist approach to privacy. Web surfers increasingly view infringements of their privacy – spamming, profiling,

[78] Article 3 – Illegal interception:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

[79] See, in this context, the excellent article by Léonard, 'E-commerce et protection', above n. 35.

[80] Following a class action brought against it some years ago in the US, DoubleClick's practice is now to send all non-identified terminals an initial non-residual and non-identifying cookie named 'accept cookies'. If the cookie is returned, DoubleClick assumes that the terminal accepts cookies and sends an identifying cookie that remains in place for about ten years (previously thirty). If the cookie is not returned, DoubleClick will indefinitely send the cookie requesting authorisation. An opt-out is available that enables informed users to store a cookie that signifies that they do not accept them.

differential charging policies, refusal of access to certain services and so on – from the standpoint of consumers of these new services.

Thus, in the United States the first hesitant steps towards legislation on data protection in the private sector focused on online consumer protection. We should bear in mind the 2000 report of the Federal Trade Commission,[81] which emphasised the need for privacy legislation to protect online consumers. In Europe, as in America, measures to combat spamming are concerned with both consumers' economic interests and data subjects' privacy.

This convergence between consumers' economic interests and citizens' freedoms opens up interesting prospects. It suggests that the right to resort to certain forms of collective action, which is already recognised in the consumer protection field, should be extended to privacy matters. Such an entitlement to 'class actions' is particularly relevant in an area where it is often difficult to assess the detriment suffered by data subjects and where the low level of damages awarded is a disincentive to individual actions. In addition, many other aspects of consumer law could usefully be applied to data protection. Examples are: the obligations to provide information and advice, which could be imposed on operators offering services that essentially involve the management or supply of personal data, such as internet access providers and personal database servers (case law databases, search engines and so on); the law governing general contractual conditions; and measures to combat unfair commercial practices and competition.

Providing personal data as a condition of access to a site or an online service could be viewed not merely from the standpoint of data protection legislation – does the user's consent meet the necessary requirements and is it sufficient to legitimise the processing in question? – but also from that of consumer law, if only in terms of unfair practices in obtaining consent or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied. Another avenue to be explored is whether consumer product liability for terminals and software

[81] US, Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on 'Privacy Online: Fair Information Practices in the Electronic Marketplace'* (May 2000), available from http://www.ftc.gov/os/2000/05/index.htm. In the US, the Federal Trade Commission, which is very active in the consumer protection field, has played a key role in protecting citizens' privacy. On that issue, see Jan Dhont and María Verónica Perez-Asinari, 'New Physics and the Law: A Comparative Approach to the EU and US Privacy and Data Protection Requirement – Looking for "Adequate Protection"' in F. van der Mensbrugghe (ed.), *L'utilisation de la méthode comparative en droit européen – Usage of Comparative Methodology in European Law* (Belgium: Presses Universitaires de Namur, 2003).

can be extended beyond any physical and financial harm caused to include infringements of data protection requirements. How far is the supplier of browser software whose use leads to breaches of privacy objectively liable for data infringements by third parties?

Conclusions

The debate about privacy and the internet is crucial because of the new risks created by the wide reach and the very characteristics of the internet itself. To address these risks a re-evaluation of the basic principles of legislation is required and new legislation may even be needed to keep up with development and the convergence of technologies. More importantly, new fields of investigation need to be opened up as it becomes clear that legislation can no longer provide all the answers. On the one hand, self-regulation is certainly a complementary source that allows various professional *milieus* (the world of cyber marketing, of access providers, of research services or network operators) to develop more specific solutions that build upon the more general or vague principles in the legislation. These solutions, whether at a national, regional or international level, should be developed, as much as possible, in concert with the other interested actors: consumer representatives, civil liberties associations, and so forth. On the other hand, when looking towards the future, technical norms may well provide the optimal mechanism for locating solutions that display respect for everyone's freedom of choice and privacy. In this regard, it is the responsibility of the authorities charged with data protection to penetrate the forums where important decisions are being taken about technical network infrastructure, communication protocols and the characteristics of our browsers.[82]

We are entering a new generation of privacy laws which must be characterised by the recognition of the technology itself as a third party between data controllers and data subjects. The use of new technologies multiplies the amount of data and the individuals capable of accessing it, increases the power of those who collect and process it, and bridges frontiers. A further factor to be taken into account is the complexity and opacity of this technology. A third party – be it the terminal or the network – now intervenes between individual and data controller. Informational

[82] More and more the specifications of the networks' and terminal functioning are defined by international private organisations without oversight or control by the governments, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN) or the World Wide Web Consortium (W3Consortium).

self-determination calls for a measure of control over this third party. So we underline the need for the internet users to understand and control their ICT environment and for society to control and anticipate the technological developments.

Ideally, these debates should take place at a global rather than national level. The internet is global and as time passes the futility of purely national legislative action becomes clearer. The search for an international consensus is evident. To achieve this, privacy advocates could benefit from the support of new pressure groups such as rights organisations and, especially, consumer organisations. In sum, the debate about privacy and the internet has only just begun. Its significance equals that of the internet itself: it is both global and essential if our freedoms are to survive in everyday life.